

CONTACT HOURS: 40 hours

CEUs: 4

PDU: 40

DELIVERY MODE: Online self-paced

TRANSFERABILITY: N/A

GRADING CRITERIA: N/A

EVALUATIONS: Learners must achieve an average test score of at least 70% to meet the minimum successful completion requirement and qualify to receive IACET CEUs.

The following list outlines the PDUs you will earn for completing this course, based on the certification you have.

Designation	Technical	Leadership	Strategic/Business	TOTAL
PMP®/PgMP®	23.5	5	11.5	40
PMI-RMP®	23.5	5	11.5	40
PMI-SP®	0	5	11.5	16.5
PMI-ACP®	23.5	5	11.5	40
PfMP®	0	5	11.5	16.5
PMI-PBA®	0	5	11.5	16.5

STUDENT RESPONSIBILITIES: Completion of any practice lessons, quizzes, assignments, or tests.

COURSE SCHEDULE/TENTATIVE TIMELINE:

Dates vary (refer to website for current availability).

LEARNING OUTCOMES:

Upon successful completion of this course, learners will be able to:

- Discuss the foundational concepts of information security, such as the CIA triad
- Know the different information security frameworks
- Explain information security training and education
- Discuss the information life cycle
- Explain how information and data are classified
- Learn about data and information privacy

- Understand system and computer architecture
- Explain and compare symmetric and asymmetric cryptography
- Learn about physical security risks and mitigation
- Compare different types of networks
- Contrast the OSI model with the TCP/IP Model
- Identify and differentiate among network, routing, and data link protocols
- Describe the functions of common networking devices and how wireless networks work
- Evaluate different identification methods and technologies
- Assess and test various security controls
- Describe business continuity and disaster recovery plans
- Understand the role of security operations
- Identify trusted recovery techniques
- Relate the steps required in effective incident management
- Discuss the role of auditing, monitoring, and detection in information security
- Learn the steps of a digital forensics investigation
- Explain the software development life cycle
- Discuss the role of databases in information security
- Recognize several software-based and network attacks